

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

JULIANNA FELIX GAMBOA, et al.,
Plaintiffs,
v.
APPLE INC.,
Defendant.

Case No. [24-cv-01270-EKL](#) (VKD)

**ORDER RE DISPUTE REGARDING
PROPOSED PROTECTIVE ORDER**

Re: Dkt. No. 35

Plaintiffs Julianna Felix Gamboa and Thomas Dorobiala (“plaintiffs”) and defendant Apple Inc. (“Apple”) have agreed to request entry of a two-tier protective order that provides for the exchange of discovery material designated “Confidential” or “Highly Confidential – Attorneys’ Eyes Only” (“HC-AEO”). Dkt. No. 35-1 at 9, 11; Dkt. No. 35-4 at 8, 10. They ask the Court to resolve their disputes regarding certain provisions in the proposed order. Dkt. No. 35. The Court finds this matter suitable for resolution without oral argument. Civil L.R. 7-1(b).

The Court addresses each disputed provision below.

1. Data Security Protocols (sec. 11(a))

In section 11 of the proposed protective order, the parties agree that they should be required to “implement an information security management system (“ISMS”) to safeguard Protected Materials, including reasonable and appropriate administrative, physical, and technical safeguards, and network security and encryption technologies governed by written policies and procedures.” Dkt. No. 35-1 at 14; Dkt. No. 35-4 at 12-13. They disagree about whether compliance with one or more specific, standard protocols should be required.

Citing a recent increase in cyberattacks against law firms and other litigation participants,

1 Apple argues that the Court should adopt a provision that requires the parties to comply “with at
2 least one of the then-current versions of the following standards: (a) the International Organization
3 for Standardization’s 27001 standard; (b) the National Institute of Standards and Technology’s
4 (NIST) 800-53 standard; (c) the Center for Internet Security’s Critical Security Controls; or (d) the
5 most recently published version of another widely recognized industry or government
6 cybersecurity framework.” Dkt. No. 35-4 (sec. 11(a)). Plaintiffs argue that the protections Apple
7 advocates are unnecessary and onerous, given the nature of the case and the documents and
8 information likely to be exchanged in discovery, and they propose instead a modified version of
9 the existing provisions in the District’s model protective order. *See* Dkt. No. 35-1 (sec. 11(a), (b)).

10 In this action, plaintiffs allege that Apple has engaged in anticompetitive conduct by
11 requiring consumers who use Apple mobile devices to use iCloud to back up and store certain
12 files, and by monopolizing (and attempting to monopolize) the market for “full-service” cloud
13 storage on Apple mobile devices. *See* Dkt. No. 24 ¶¶ 9-12. Apple focuses on the need to
14 “preserve the security of consumer and confidential business data.” Dkt. No. 35 at 5; *see also id.*
15 at 10-11. However, the Court anticipates that little, if any, user-specific or personally identifiable
16 information, will be produced in discovery, and that any relevant consumer data can be provided
17 in anonymized and/or aggregate form. Similarly, the business data subject to discovery is likely to
18 be no different here than in any other antitrust case. Apple does not identify any specific
19 discovery material that is particularly sensitive or particularly vulnerable; indeed, Apple’s
20 proposed provision would apply to *all* Protected Materials, whether designated “HC-AEO” or
21 “Confidential.”

22 As Apple has not demonstrated that compliance with one or more of the strict, standard
23 protocols listed in its proposed provision is necessary here, the Court adopts plaintiffs’ proposal:

24 Receiving Party shall implement an information security
25 management system (“ISMS”) to safeguard Protected Materials,
26 including reasonable and appropriate administrative, physical, and
27 technical safeguards, and network security and encryption
28 technologies governed by written policies and procedures designed
to protect against any reasonably anticipated threats or hazards to
the security of such Protected Material and to protect against
unauthorized access to Protected Material. To the extent a party or

1 person does not have an ISMS, they may comply with this provision
2 by having the Protected Material managed by and/or stored with
3 eDiscovery vendors, claims administrators, or other platforms that
4 maintain such an ISMS.

Dkt. No. 35-1 (sec. 11(a)).

5 **2. Multi-Factor Authentication (sec. 11(a))**

6 The parties agree that multi-factor authentication and encryption should be used to prevent
7 unauthorized access to Protected Materials. They appear to disagree regarding the particular
8 implementation of multi-factor authentication, although the nature of that disagreement is
9 somewhat unclear.

10 The Court adopts Apple’s proposal, with one modification (in italics):

11 The Parties shall implement multi-factor authentication for any
12 access to Protected Materials. *At a minimum, multi-factor*
13 *authentication must be implemented on a device-specific basis but*
14 *need not be implemented on a document-specific basis.* The parties
15 shall implement encryption of all Protected Materials (i) in transit
16 outside of network(s) covered by the Party’s ISMS (except as
17 necessary to submit documents to the court in accordance with
18 Section 13 below) and (ii) at rest where reasonably practical.

16 To the extent Apple advocates for a document-specific multi-factor authentication requirement,
17 the Court rejects that requirement as unduly burdensome and unnecessary, in view of the
18 considerations discussed above.

19 **3. Data Breach Remediation (sec. 11(b)-(f))**

20 The parties agree that the protective order should include section 16, a provision governing
21 inadvertent or unauthorized disclosure of any “Discovery Material” (i.e. any discovery material
22 produced in the case, and not just “Protected Material”). *See* Dkt. No. 35-1 (sec. 16); Dkt. No. 35-
23 4 (sec. 16). Section 16 requires a party to (1) “immediately notify” a producing party of the
24 disclosure, (2) provide “all known relevant information concerning the nature and circumstances
25 of the disclosure,” and (3) “promptly take all reasonable measure to retrieve the improperly
26 disclosed Discovery Material and to ensure that no further or greater unauthorized disclosure
27 and/or use thereof is made.” *Id.*

28 Separately, as part of section 11, the parties describe more rigorous procedures that would

1 apply to Protected Material only. They disagree about the circumstances in which such
2 procedures must be used, and about some of the specific procedures. Apple argues that “any
3 unauthorized access, use, or disclosure of Protected Materials or devices containing Protected
4 Materials” should be considered a “Data Breach,” and that Apple’s more rigorous procedures
5 should apply. Dkt. No. 35 at 9; Dkt. No. 35-4 (sec. 11(b)). Plaintiffs argue that the requirements
6 of section 16 are sufficient to address accidental or harmless unauthorized disclosures and that
7 plaintiffs’ more rigorous procedures should apply only in the event of a “cyberattack or other
8 deliberate security breach resulting in actual or potential unauthorized access to Protected
9 Materials.” Dkt. No. 35 at 5; Dkt. No. 35-1 (sec. 11(b)).

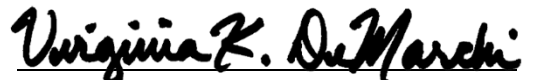
10 The Court agrees with plaintiffs that, as a general matter, the provisions of section 16 are
11 sufficient to protect a party’s interests in the event of an inadvertent or unauthorized disclosure of
12 Protected Material. However, those provisions may not be sufficient in the event of a deliberate
13 security breach, where immediate action, additional investigation, and more rigorous remediation
14 measures may be necessary. Thus, the Court adopts plaintiffs’ proposal as reflected in sections
15 11(b)-(f), as that proposal appropriately distinguishes between these circumstances.

16 ***

17 The parties shall file a proposed protective order that conforms to the Court’s decision of
18 the disputed issues presented. In addition, the parties are advised that any discovery disputes,
19 including challenges to designations of Protected Material, are subject to the Court’s discovery
20 dispute procedures described in Judge DeMarchi’s Standing Order for Civil Cases, available at
21 <https://cand.uscourts.gov/standing-order-for-civil-cases-april-2024/>. The parties’ proposed
22 protective order should so state.

23 **IT IS SO ORDERED.**

24 Dated: November 26, 2024

25
26 
27 Virginia K. DeMarchi
28 United States Magistrate Judge